1. (currently amended) A computer authentication protocol, comprising:

sending at least one certificate payload from a transmitting computer to a receiving computer, the certificate payload including at least two certificates each being generated by a respective certificate authority (CA), the certificate authorities being independent of each other such that no trust relationship exists between the CAs.

2. (original) The protocol of claim 1, wherein the certificates are concatenated together.

3. (original) The protocol of Claim 2, wherein at least one certificate is associated with a person and one certificate is associated with a host computer.

4. (original) The protocol of Claim 1, further comprising sending at least one identification (ID) payload between the computers, the ID payload being generated by combining the IDs of at least two entities.

5. (original) The protocol of Claim 4, further comprising sending at least one signature payload between the computers, the signature payload being generated by concatenating the signatures of at least two entities.

6. (currently amended) The protocol of Claim 4 5, wherein each signature is formed by applying a pseudorandom function (PRF) to at least the associated ID to render a result, and then encrypting the result with a private key associated with the entity represented by the ID.

7. (original) A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer, comprising:

logic means for combining a first entity identification (ID) with a second entity ID to render an ID payload; and

logic means for sending the ID payload to a computer along with at least one certificate payload.

8. (original) The computer program device of Claim 7, further comprising:

logic means for generating a signature payload by concatenating at least two signatures of respective entities.

9. (original) The computer program device of Claim 8, wherein the means for generating a signature payload applies a pseudorandom function (PRF) to at least an ID associated with an entity to render a result, and then encrypting the result with a private key associated with the entity represented by the respective ID.

10. (original) A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer, comprising:

logic means for generating a signature payload by concatenating at least two signatures of respective entities; and

logic means for sending the signature payload to a computer along with at least one certificate payload.

11. (original) The computer program device of Claim 10, wherein the means for generating a signature payload applies a pseudorandom function (PRF) to at least an ID associated with an entity to render a result, and then encrypting the result with a private key associated with the entity represented by the respective ID.

12. (original) The computer program device of Claim 11, further comprising:

logic means for combining a first entity ID with a second entity ID to render an ID payload; and

logic means for sending the ID payload to a computer along with at least one certificate payload.

13. (original) A computer system for secure network authentication, comprising:

at least one host certificate authority (CA) generating a host authentication certificate for at least one host computer; and at least one user CA generating a user authentication certificate for at least one user, wherein the certificates can be combined into a certificate payload during an authentication process, the host CA not being in a trust relationship with the user CA and vice-versa.

14. (original) The system of claim 13, wherein the certificates are concatenated together to establish a certificate payload.

15. (original) The system of Claim 14, wherein at least one certificate is associated with a person and one certificate is associated with a host computer.

16. (original) The system of Claim 13, wherein the system sends at least one identification (ID) payload between the computers, the ID payload being generated by combining the IDs of at least two entities.

17. (original) The system of Claim 16, wherein the system sends at least one signature payload between the computers, the signature payload being generated by concatenating the signatures of at least two entities.

18. (original) The system of Claim 17, wherein each signature is formed by applying a pseudorandom function (PRF) to at least the associated ID to render a result, and then encrypting the result with a private key associated with the entity represented by the ID.